IB03/04178

19.09.03

10/527706

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

I documenti allegati sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 17. SEP. 2003

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

H. Jenni

Heinz Jenni

Demande de brevet no 2002 1595/02

CERTIFICAT DE DEPOT (art. 46 al. 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous.

Titre:
Système de filigrane numérique à modulation asymétrique robuste à un sous échantillonnage spatial.

Requérant:
AlpVision SA
Rue du Clos 12
1800 Vevey

Date du dépôt: 20.09.2002

Classement provisoire: G09C

Enregistrement mandataire:
Leman Consulting S.A.
Route de Clémenty 62
1260 Nyon
(mandataire)

reg: 16.09.2003

Système de filigrane numérique à modulation asymétrique robuste à un sous échantillonnage spatial

DESCRIPTION

Domaine technique

Le domaine général concerne une technique de traitement du signal et d'image permettant de camoufler de informations de manière invisible dans des médias digitaux (image, vidéo, son) ou analogiques (imprimé).

Un filigrane numérique à modulation asymétrique est une extension des filigranes numériques classiques. Cette extension permet en particulier de couvrir les médias imprimés en offrant une solution pour imprimer de manière invisible un filigrane numérique sur un média de couleur uniforme avec une encre de couleur visible. Le domaine d'application concerne la sécurisation des documents et emballages imprimés contre la contrefaçon et la falsification.

Etat de la technique

Les systèmes usuels destinés à prévenir la contrefaçon ou l'altération de documents imprimés ou gravés peuvent être classés en différents groupes:

- les hologrammes, les impressions de motifs spéciaux
- les impressions avec encres spéciales ou code à encre invisibles
- les systèmes à puce ou antennes

Les hologrammes, motifs spéciaux et autres décorations sont difficiles à reproduire car leur réalisation nécessite un équipement spécial. Ils sont spécialement conçus pour interférer avec les systèmes de photocopie classique de telle sorte que la copie soit visiblement différente de l'original. Ces systèmes peuvent être contrôlés visuellement sans l'aide de dispositifs particuliers mais présentent l'inconvénient d'être coûteux, assez connus pour être reproduits sans problèmes par des experts en contrefaçon, et finalement leur visibilité nuit à l'esthétique de l'objet protégé (emballage de parfum par exemple). Leur visibilité est également la raison de leur efficacité limitée dans la mesure où un pirate peut facilement identifier l'élément de sécurité, soit pour le copier, soit pour l'effacer physiquement.

Les impressions avec encres spéciales utilisent des propriétés chimiques particulières de l'encre pour fournir une réaction déterminée à une action particulière. Ainsi, les encres fluorescentes deviennent très lumineuses quand elles

sont éclairées par une longueur d'onde particulière, certaines encres sont même invisibles à la lumière naturelle, d'autres encres changent de couleur en fonction de leur orientation ou de leur température (et peuvent se révéler en chauffant le papier avec un doigt), etc. Les encres spéciales ont comme point commun d'être particulièrement coûteuses et de nécessiter d'opérer des modifications dans la chaîne de production industrielle habituelle (masque supplémentaire pour l'offset par exemple). De plus, bien que plus robuste à la contrefaçon que le groupe précédent, il est également possible de reproduire leurs effets dans la mesure où le pirate peut contrôler par lui-même la fidélité de sa copie par rapport à l'original dès qu'il dispose du dispositif faisant réagir l'encre.

Les codes utilisant des encres invisibles, à la différence des deux groupes précédents, permettent de cacher une information numérique. Ces codes peuvent être des caractères, des codes barres, des codes 2D, etc. En plus de son coût élevé et propre aux encres invisibles, ce système a deux inconvénients majeurs. D'une part, du fait de la nature des codes utilisés, il est localisé sur une certaine partie du document ou de l'emballage et il est donc possible de le détruire sans altérer la totalité de la surface. D'autre part, les codes utilisés ont toujours des particularités géométriques (barres, figures géométriques, caractères, etc) les identifiant clairement comme des dispositifs anti-copie. Cela facilite grandement la tache du pirate cherchant à révéler et à reproduire l'encre. De plus dès que le pirate sait réaliser cette reproduction, il détient ipso facto le moyen de reproduire le code. Finalement les systèmes basés sur des mémoires ou processeurs embarqués cumulent les inconvénients d'être très coûteux, inesthétiques et localisés. Leur application principale consiste plus à sécuriser une communication, ou à stocker dynamiquement une information plutôt qu'à distinguer un original d'une copie.

La technique du filigrane numérique, également connue sous le nom de tatouage numérique, est une technique permettant de *cacher* des informations de manière *robuste et imperceptible* dans des données multimédia telles que la musique, la vidéo, les images, les documents, etc. L'information qui est cachée s'appelle la *signature*. Cette signature peut être par exemple un numéro, un nom ou même une

image. Après la protection des données multimédia avec un filigrane numérique on parle d'image signée, de vidéo signée, etc.

De nombreuses publications ont été faites sur les différentes techniques permettant de cacher un filigrane dans une image, dans une vidéo ou un signal audio. En ce qui concerne les images, ces dernières peuvent se classer en fonction de la technique utilisée pour le marquage : certaines opèrent des modifications directement dans le domaine spatial (voir par exemple [1] M. Kutter, F. Jordan, F. Bossen, "Digital watermaking of color images using amplitude modulation", *Journal of Electronic Imaging*, vol. 7, n° 2, pp. 326-332, April 1998.), d'autres opèrent ces modifications dans un domaine transformé (par exemple le domaine fréquentiel) voire des domaines intermédiaires comme les ondelettes (voir [2] Shelby Pereira, Sviatoslav Voloshynovskiy and Thierry Pun, Optimized wavelet domain watermark embedding strategy using linear programming, In Harold H. Szu and Martin Vetterli eds., *Wavelet Applications VII (part of SPIE AeroSense 2000)*, Orlando, Florida USA, April 26-28 2000.).

Le procédé décrit dans le brevet numéro WO0225599 (priorité CH20000001832 20000920) étend la technologie de filigrane numérique à un média imprimé, par une modulation asymétrique d'un signal indépendant du support sous-jacent et plus connue sous le terme de cryptoglyph. Parmi les intérêts de cette approche, on peut citer l'impression invisible sur du papier de couleur uniforme (blanche en particulier), ou la surimpression sur des imprimés (obtenus en offset en particulier). La détection de ce signal requiert un scanner numérique. Une contrainte notable de cette approche est que le scanner numérique doit avoir au moins la même résolution que celle utilisée pour imprimer le signal.

La présente invention décrit un procédé permettant de s'affranchir de cette contrainte et permettant donc d'utiliser un scanner basse résolution pour détecter un cryptoglyph imprimé à haute résolution.

Description détaillée de l'invention

Un cryptoglyph se présente comme un nuage de points à répartition spatiale pseudo aléatoire. Dans ce qui suit on définit « la résolution d'impression » sur la base de la taille effective du cryptoglyph une fois imprimé rapporté à sa taille en

pixel, et non pas comme la densité maximale de points par unité de longueur que peut fournir l'imprimante.

Afin d'illustrer, le caractère critique des résolutions respectives d'impression et de numérisation, un exemple est donné dans ce qui suit pour le cas particulier de la détermination du positionnement vertical de deux points. Lorsque le cryptoglyph est imprimé à une résolution de *d* point par unité de longueur, la taille des points a un diamètre de l'ordre de 1/*d*. Une numérisation de ces points peut être accomplie avec un scanner possédant un résolution *d* comme indiqué à la Figure 2 : la taille des points imprimés étant identiques à la résolution du numériseur, il est possible de les discriminer (le point du bas se situe à droite du point du haut). Dans le cas d'une numérisation réalisée à une résolution inférieure (par exemple deux fois inférieure), une telle discrimination est théoriquement impossible, comme indiqué à la Figure 1. Dans ce cas, on voit que le numériseur digitalise les deux points comme appartenant à la même ligne. Le même raisonnement est également valide pour la résolution horizontale de l'image. Cette limitation semble donc être fondamentalement intrinsèque à la technologie du cryptoglyph et il était jusqu'ici admis que le résolution de numérisation ne pouvait en aucun cas être inférieure à celle d'impression.

Le procédé suivant montre néanmoins qu'une telle possibilité existe : une solution consiste à espacer les points de manière à compenser exactement la différence de résolution entre impression et numérisation comme illustré à la Figure 3. Dans ce cas, des lignes supplémentaires vides ont été insérées permettant un espacement vertical des points de *2/d*.

L'avantage notable de cette invention est qu'elle permet de détecter un cryptoglyph avec les nombreux systèmes basés sur des scanners digitaux à basse résolution. C'est le cas en particulier des numériseurs à haut débit utilisés pour les documents papier (chèques, virements bancaires, etc.) mais aussi de certains lecteurs de carte.

Un autre avantage du système est qu'il permet d'augmenter l'invisibilité du cryptoglyph en utilisant les deux phénomènes suivants :

- Diminution de la taille des points
- Diminution de la concentration de points par unité de surface imprimée

Ces paramètres sont mathématiquement quantifiés ci-dessous.

Liste des dessins

Figure 1: Représentation du signal et de la zone numérisée par un scanner d'une résolution deux fois plus basse que la taille des points.

Figure 2 : Représentation du signal et de la zone numérisée par un scanner de résolution identique à la taille des points.

Figure 3: Utilisation d'une résolution de numérisation plus basse que celle d'impression.

Figure 4 : Illustration du changement de l'espacement pour la dimension verticale et horizontale.

Figure 5 : Diagramme du procédé permettant d'obtenir un cryptoglyph sur échantillonné et érodé.

Figure 6 : Diagramme de la mise en œuvre du cryptoglyph modifié pour l'impression et la détection.

Figure 7 : Calcul de l'assombrissement relatif d'un point après post traitement et numérisation.

Réalisation de l'invention

Une méthode de réalisation de l'invention est basée sur un procédé de post traitement d'une image de cryptoglyph illustré par le diagramme de la Figure 5. Un cryptoglyph standard à répartition pseudo aléatoire d'une taille $x \times y$ est d'abord généré. Ce dernier est ensuite sur échantillonné de manière binaire d'un facteur n dans ses dimensions horizontales et verticales par le module (1). Le résultat est un cryptoglyph de taille $nx \times ny$ dont en particulier les points encodant le signal - porteurs de l'information redondante - font désormais une taille de $n \times n$. Cette image est ensuite retraitée au moyen d'un filtre érosif (2) conduisant à des points à nouveau d'une taille de 1x1 mais dans une image faisant toujours $nx \times ny$. Ce procédé est ainsi qualifié de « sur échantillonnage érosif ».

La mise en œuvre de l'impression et détection du cryptoglyph ainsi obtenu est illustrée par la Figure 6. Dans une première étape (3), le cryptoglyph est tout d'abord imprimé avec une résolution $d1$. Le support imprimé ainsi obtenu est subséquemment numérisé (4) avec une résolution $d2$. Comme mentionné précédemment, l'objet de la présente invention est précisément que $d2 < d1$.

Il existe une relation liant mathématiquement le procédé de post traitement à la mise en œuvre du cryptoglyph. Cette dernière est donné par :

$$n = \frac{d_1}{d_2}$$

La numérisation avec une résolution $d2$ du cryptoglyph post traité conduit à une diminution du contraste entre les points et le fond qui dépend du rapport n. La couleur finale du point peut être calculée par moyenne. Soit b la couleur de fond et c la couleur des points du cryptoglyph, la couleur finale des points est alors :

$$c' = \frac{b \cdot \left(n^2 - 1\right) + c}{n^2}$$

Dans le cas particulier d'un signal noir c=0 sur fond blanc b=1, on peut constater que $c' >> c$. Le contraste du signal par rapport au fond est effectivement diminué, ce qui augmente l'invisibilité en même temps que le rapport signal bruit qui caractérise la clarté du cryptoglyph par rapport au support sur lequel il est imprimé.

La méthode décrite ci-dessus peut être généralisée aux cas d'un traitement anisotrope du cryptoglyph. Dans ce cas, les résolutions utilisées pour la numérisation et l'impression sont différentes selon les directions x et y. Comme cette méthode agit indépendamment sur chacune de ces dimensions, elle peut être appliquée directement. Les relations se généralisent alors en considérant la densité selon les directions x et y utilisées pour l'impression (resp. $d1x$ et $d1y$) et celles utilisées pour la numérisation (resp. $d2x$ et $d2y$) donnant le facteur de sur échantillonnage érosif selon les directions x et y, respectivement nx et ny :

$$nx = \frac{d_{1x}}{d_{2x}}$$

$$ny = \frac{d_{1y}}{d_{2y}}$$

Ces facteurs sont en particulier applicables dans le cas d'imprimantes industrielles à jet d'encre dont la vitesse de défilement du papier est susceptible d'engendrer une résolution différente dans les deux dimensions, un effet similaire peut également être constaté sur un scanner.

REVENDICATIONS

1. Procédé de génération d'un filigrane numérique à modulation asymétrique permettant sa détection malgré un sous échantillonnage spatial du signal.

2. Procédé selon la revendication 1, où la détection du filigrane numérique est réalisée après avoir été imprimé et numérisé.

3. Procédé selon la revendication 4, caractérisé par une résolution de numérisation inférieure à la résolution d'impression.

4. Procédé selon la revendication 1, caractérisé par un espacement des points supérieur à l'espacement minimal correspondant à la résolution d'impression.

5. Procédé selon la revendication 4, caractérisé par l'utilisation d'un procédé de sur échantillonnage suivi d'un traitement par filtrage érosif sur un filigrane traditionnel pour obtenir la diminution relative de taille des points.

6. Application du procédé selon la revendication 1 ou 4 dans le but de diminuer la quantité de calculs nécessaire à la détection.

7. Application du procédé selon la revendication 1 ou 4 dans le but de diminuer la visibilité du filigrane numérique asymétrique.

8. Procédé selon la revendication 1 ou 4, caractérisé par des fréquences d'échantillonnage différentes selon les directions horizontales et verticales.

9. Application du procédé selon la revendication 8, pour permettre la compatibilité avec des matériels d'impression ou de numérisation anisotropes.

ABREGE

L'invention décrit un procédé permettant la détection de cryptoglyph à l'aide d'un dispositif de numérisation dont la résolution est inférieure à celle utilisée pour l'impression. Le procédé repose sur un traitement particulier de l'image du cryptoglyph permettant de diminuer la taille relative des points qui le composent.

DESSINS

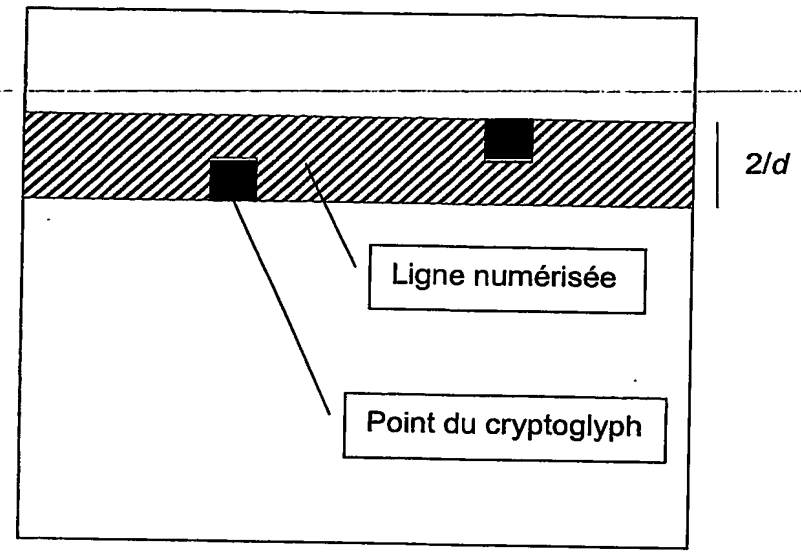


Figure 1: Représentation du signal et de la zone numérisée par un scanner d'une résolution deux fois plus basse que la taille des points.

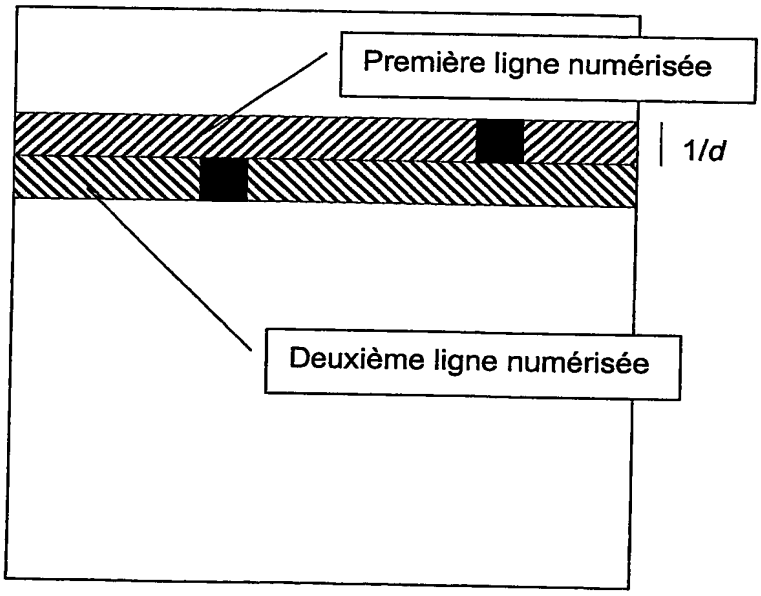


Figure 2 : Représentation du signal et de la zone numérisée par un scanner de résolution identique à la taille des points.

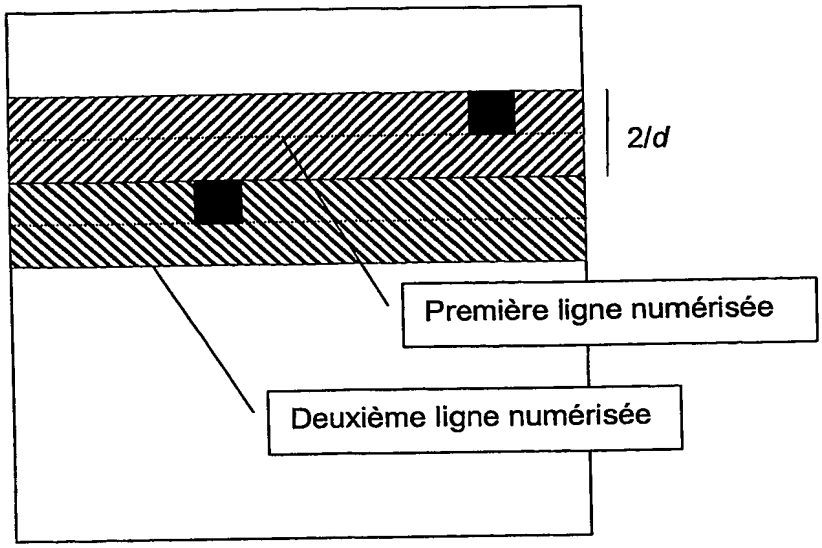


Figure 3: Utilisation d'une résolution de numérisation plus basse que celle d'impression.

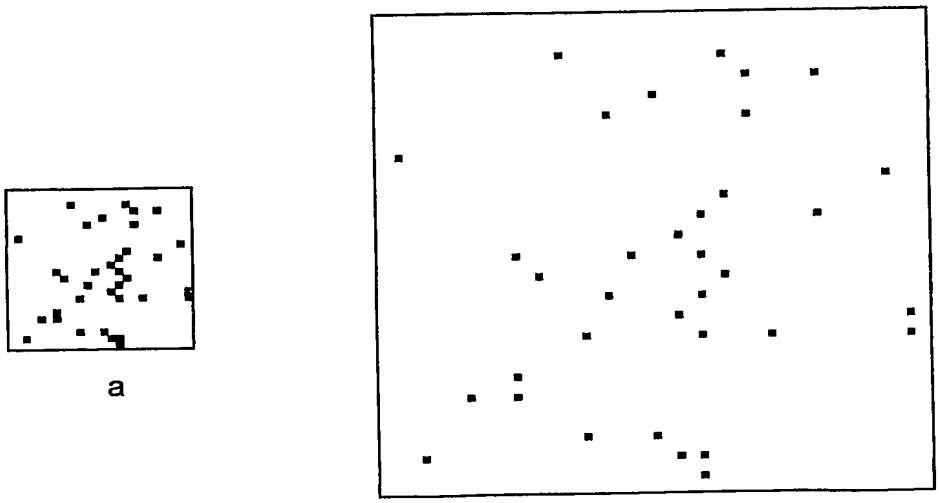


Figure 4 : Illustration du changement de l'espacement pour la dimension verticale et horizontale.

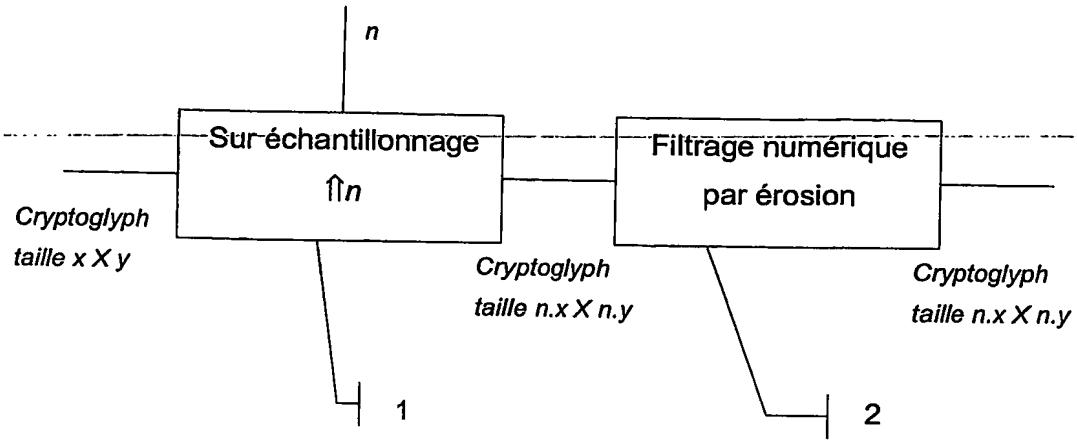
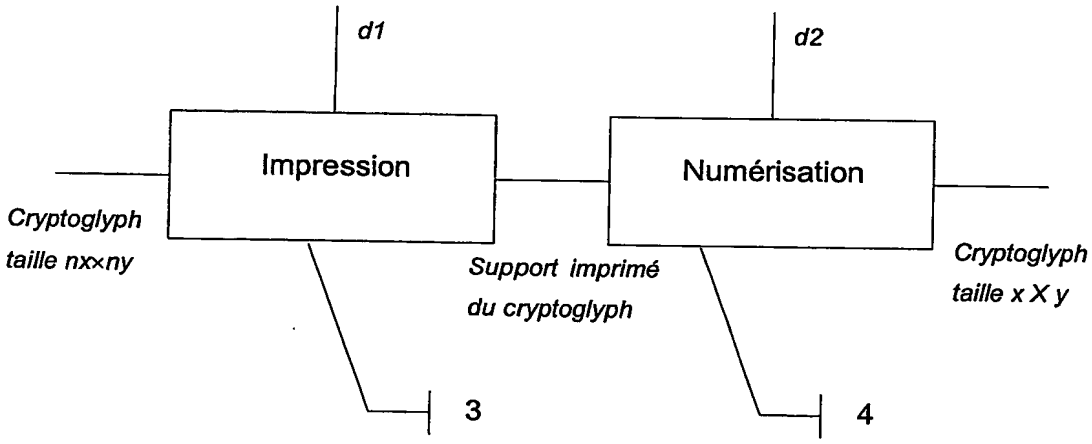


Figure 5 : Diagramme du procédé permettant d'obtenir un cryptoglyph sur échantillonné et érodé.



5 Figure 6 : Diagramme de la mise en œuvre du cryptoglyph modifié pour l'impression et la détection.

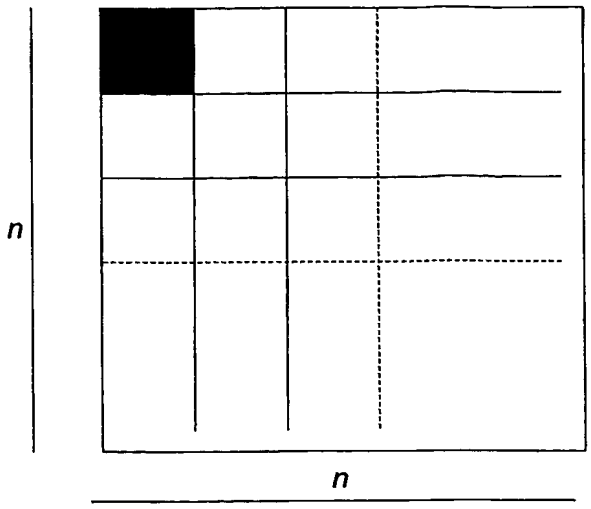


Figure 7 : Calcul de l'assombrissement relatif d'un point après post traitement et numérisation.